BULLETIN DROIT & BANQUE

EXTRAIT 67

BULLETIN

DROIT & BANQUE

N° 67

Décembre 2020

Editeur:

Association Luxembourgeoise des Juristes de Droit Bancaire a.s.b.l.

www.aljb.lu

Secrétariat, Inscriptions:

secretariat@aljb.lu
House of Finance
B.P. 13
L-2010 Luxembourg

Tokenised securities in Luxembourg: concept and legal considerations to be taken into account upon an issuance

Karl Pardaens[1]
Avocat à la Cour
Elvinger Hoss Prussen

Benoît Nerriec
Juriste, member of the New York Bar
Elvinger Hoss Prussen

*DLT, blockchain and security tokens are hot topics among legal authors and numerous publications have been made to date. Distributed ledger technology ("**DLT**") is increasingly used by businesses in different sectors, with many Fintech start-ups flourishing in Luxembourg and Europe. In Luxembourg, the Commission de Surveillance du Secteur Financier (the "**CSSF**") has over the last couple of years been contacted by numerous promoters of projects involving DLT and gained expertise in relation thereto*[2]*, without however releasing extensive guidelines or analyses, unlike e.g. the AMF*[3] *or BaFin*[4]*. The Luxembourg legislator has been active in the same period with some amendments made to its legislation to take into account DLT. However, we currently see a gap between this new technology which attracts an increasing number of actors willing to use it and the absence of clear legislative framework regulating the issuance of tokens, in particular those qualifying as financial instruments (the so-called security tokens). Nevertheless, Luxembourg law does not prevent the tokenisation of traditional securities (and more specifically securities in registered form) which will be the focus of this paper. The objective of this paper is to draw the attention on different legal considerations to take into account when contemplating an issuance of tokenised securities.*

As we write this paper[5]*, the European Commission has finally launched its digital finance strategy with different proposals that we will briefly touch upon. This is an important step towards the digital transformation of the economy and the financial industry and will lead market actors, regulators and supervisors to work together in order to create a sound legal framework within the European Union. We can also anticipate that the launch of the digital finance strategy will lead to the introduction of new regulations under Luxembourg law which, one may hope, will create an attractive legal framework for Fintech actors and will continue to position Luxembourg as a leader in digital finance in Europe.*

1 The views expressed in this paper are those of the authors and do not necessarily reflect the views of the law firm Elvinger Hoss Prussen, *société anonyme*.

2 CSSF Annual Report 2019, p.32 (https://www.cssf.lu/en/2020/09/publication-of-the-cssfs-annual-report-2019).

3 Autorité des marchés financiers, the financial regulatory authority for France (see in particular, "Synthèse des réponses à la consultation publique portant sur les Initial Coin Offerings (ICO) et point d'étape sur le programme "Unicorn"" (https://www.amf-france.org/fr/actualites-publications/consultations-publiques/synthese-des-reponses-la-consultation-publique-portant-sur-les-initial-coin-offerings-ico-et-point) and "Etat des lieux et analyse relative à l'application de la réglementation financière aux security tokens " (https://www.amf-france.org/fr/actualites-publications/actualites/analyse-juridique-sur-lapplication-de-la-regle-mentation-financiere-aux-security-tokens-et-precisions).

4 Bundesanstalt für Finanzdienstleistungsaufsicht, the financial regulatory authority for Germany (see in particular, "Initial Coin Offerings: Advisory letter on the classification of tokens as financial instruments", 28 March 2018 (https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.html;jsessionid=549E6A96822084BE260F98A148143973.2_cid393?nn=11089708) and "Second advisory letter on prospectus and authorization requirements in connection with the issuance of crypto tokens", 22 November 2019 (https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_wa_merkblatt_ICOs_en.html).

5 This paper was written as of 10 October 2020.

Table of Contents

I. DLT and the issuance of tokenised securities

In order to fully understand what entails an issuance of tokenised securities and distinguish it from an issuance of tokens only, one must first understand how DLT functions and we consider that in that context, some clarifications should also be made as regards the legal terminology associated with DLT (A). We will then turn to what issuers will need to consider when issuing tokenised securities, in particular, in terms of securities that can be tokenised and arrangements necessary for the tokenisation process to occur (B).

A) General considerations on DLT and legal terminology

To understand the legal issues that companies and issuers may face when using DLT, it is important to first explain, in layman's terms, certain technological concepts and clarify the terminology which is often not correctly or heterogeneously used and can lead to confusions if readers are not familiar with this technology[6]. The objective of the following developments is to provide the readers with some useful and simplified explanations on how DLT and tokenisation work but should not be viewed as an exhaustive overview of how this technology functions (1). In the second part of this section, we will attempt to clarify the legal terminology used in respect of tokens, in particular in light of the recent proposals of regulation made by the European Commission (2).

1. A brief introduction to DLT

We will briefly present how the technology works and key concepts associated with that technology (a) before introducing the notions of coins and tokens from a technological perspective (b).

a) DLT: DLT is not a new technology but a combination of existing technologies. Put in simple terms a DLT is a distributed database or ledger using cryptography. Blockchain constitutes one specific type of DLT[7], but it is the DLT most frequently referred to in legal publications[8] because it is the most

6 J. Lee and F. L'heureux, "A Regulatory Framework for Cryptocurrency", E*uropean Business Law Review 31, no.3 (2020): 423-446*, paragraph 4.1.2.

7 For completeness, we note that two main categories of distributed ledgers exist: the private or permissioned blockchains, which put certain conditions to access the network and to become a node, and the public or permissionless blockchains, which can be accessed by anyone.

8 G. Cywie, "La numismatisation de l'économie", *Droit du financement de l'économie, Legitech, December 2018* ; G. Canivet, "Blockchain et régulation", S*emaine Juridique – Entreprises et Affaires n°36, 7 September 2017* ; D. Legeais, "Blockchain", *Jurisclasseur Commercial, March 2017* ; G. Kolifrath, M. Goupy, "Blockchain : les enjeux en droit français", *Revue internationale des services financiers*, 2017, n°4, pp.19-24 ; M. Melki, "Les mystères de la blockchain", *Recueil Dalloz, 2 November 2017, n°37* ; B. Barraud, "Les blockchains et le droit", *Revue Lamy Droit de l'immatériel, April 2018*.

simple and common form of DLT. For the purposes of this paper, we will use the term "DLT" rather than "blockchain" when referring to the underlying technology in general, however, our analysis will mainly focus on blockchain technology. DLT has become more popular among businesses in recent years because its functionalities permit to ensure the immutability, security and decentralisation of data. How does it work?

A distributed ledger is maintained on a network that has the specificity of being decentralised. The first key characteristic of DLT is indeed that it relies on a decentralised network, which means that each node[9] of the network has a copy of the ledger and can transfer information to other nodes without having to go through a central server. In addition to being decentralised, the network is distributed which is to say that all the servers and computers of the network are interconnected and can share information[10]. The second key characteristic of DLT is the use of cryptography. The aim of this paper is not to explain in detail what cryptography is and how it works, but to set out certain underlying concepts which are essential to understand the tokenisation process.

First, the concept of hash and hash functions must be explained. Hash functions permit in essence to transform an information, transaction or a document into a fixed length series of numbers and letters which is unique to that information or document and is called a hash. In other words, the hash is the fingerprint of a document in the sense that any change in the content of that document would create a different hash. In a distributed ledger functioning as a blockchain, a block in the blockchain contains a large number of transaction data to which a specific hash is assigned. Each block of the blockchain has its own hash and the hash from the previous block which thus permits, at least in theory, to prevent any tampering in the data of the previous block. To make it more secure and avoid having hackers tampering the transaction data in one block and recalculating all the different hashes, consensus mechanisms are put in place by the participants of the blockchain to agree on the rules to be followed by the nodes to accept new entries in the blockchain. The Bitcoin Blockchain for example uses a consensus mechanism called "proof-of-work" which is "*a computational challenge that is hard to solve (in terms of computing power and processing time) but easy to verify*"[11]. That process is often referred to as "***mining***". As it takes some time to resolve the computational challenge (about 10 minutes for the Bitcoin Blockchain), it makes it much more difficult for hackers to tamper the data and change all the hashes from the previous blocks as they would need to go through that proof-of-work process for each previous block. To continue with the example of the Bitcoin blockchain, it is important to note that each person, a so-called "miner", that "*produces a valid proof-of-work in the Bitcoin network receives Bitcoins as a reward (sort of like a transaction fee), which serves as an economic incentive to maintain system integrity*[12]". However, this consensus mechanism is not the only consensus that exists. The Ethereum Blockchain, which is another well-known blockchain, is currently in the process of upgrading its blockchain with Ethereum 2.0 which will use the consensus mechanism called "proof-of-stake"[13]. With proof-of-stake, the probability to validate a new block does not depend on your computing power but on how much stake or amount of cryptocurrencies (e.g. Ether) you have[14]. The more cryptocurrencies you have deposited to validate a new block the more likely you are to validate the new block and get the transaction fee. If the new block is fraudulent[15], then the validator will lose the cryptocurrencies deposited. With proof-of-stake, the terminology is slightly different and instead of miners and mining, the terms validators and minting or forging a new block are being used. Distributed ledger technologies other than blockchain use other consensus mechanisms but they are beyond the scope of this paper.

Another concept to present is the concept of digital signature. Digital signatures are an essential part of cryptography as they permit to authenticate and identify the sender of information within the DLT while encrypting the data that is being sent. DLT is based on asymmetric cryptography which means that the digital signatures used by DLT correspond in fact to a set of two keys: a public key which is

9 A node is a participant to the network which may take several forms such as a server, a computer or even a smartphone.
10 A. Tordeurs, "Une approche pédagogique de la Blockchain", *Revue internationale des services financiers*, 2017, n°4, pp.8-18.
11 World Bank Group, "Distributed Ledger Technology (DLT) and Blockchain", *FinTech Note No.1*, 2017, p.6.
12 *Ibid*, World Bank Group, "Distributed Ledger Technology (DLT) and Blockchain", *FinTech Note No.1*, 2017, p.6.
13 For further details on the concepts of "proof-of-work" and "proof-of-stake", see for example, A. Pinna, W. Ruttenberg, "Distributed ledger technologies in securities post-trading", *European Central Bank, Occasional Paper Series No. 172, April 2016*, paragraph 2.3.
14 Additional criteria in fact come into play to determine which users will be able to participate in the forging process of a new block, including in particular the methods of "randomised block selection" and "coin age selection". These two methods (which we will not explain in this paper as it would be too technical) permit to avoid a situation where the consensus mechanism would rely solely on the wealth of the different nodes of the network, which could cause some issues if certain nodes were to own large stakes of coins.
15 This may occur in the event that the new block contains illegitimate or invalid transactions or if there is an attempt to create a fork. In such cases, the network will not validate the new block.

known by all the participants of the network and therefore permits to identify the sender of data[16], and a private key which is personal to each individual user and is used to sign and encrypt the data sent to the network[17]. Each public key is uniquely linked to a private key by a mathematical algorithm. Thus, a public key uniquely corresponds to a given private key. To give an example, a user A willing to send a message or information to a user B will send such message or information in an encrypted form using its private key and the public key of user B, and user B will in turn be able to decrypt the message with its own private key and user A's public key. User A does not need to know the private key of user B to send its message and no central counterparty is required to validate the transaction. The transaction between A and B will be validated by the participants to the blockchain through the relevant consensus mechanism and will then be added to a block of transactions that all participants to the blockchain will include in their own record or copy of the blockchain.

It is therefore essential that public and private keys be kept and stored safely by each individual user, especially private keys since it is not possible from a technical perspective to recreate the private key with the public key. This is the reason why wallet service providers offer a number of services in relation to public and private keys, and in particular, for their safe custody. As explained by the European Securities and Markets Authority ("**ESMA**"), in its advice on initial coin offerings and crypto-assets dated 9 January 2019, "*digital crypto-asset wallets are used to store public and private keys and to interact with DLTs to allow users to send and receive crypto-assets and monitor their balances. Crypto-asset wallets come in different forms. Some support multiple crypto-assets/DLTs while others are crypto-asset/DLT specific*"[18]. As further discussed in section II) A)2.b) below, it is therefore crucial to ensure that wallets are compatible with the underlying blockchain and the smart contract generating the tokens. It is also important to clarify that a wallet used in the context of a blockchain does not contain the tokens held by a particular user but only his or her public and private keys.

With this brief overview of the technology, the concepts of coins and tokens can be introduced.

b) Coins and tokens: coins and tokens should not be used interchangeably as there is a technological difference between them[19]. A coin is an asset or unit of value that is native from a specific blockchain, such as Bitcoin which is the coin native from the Bitcoin Blockchain or Ether for the Ethereum Blockchain. Tokens on the other hand do not have their own blockchain and are built on top of existing blockchains. They are generated and created through a smart contract that is built on the blockchain and permits to automatically execute transactions in accordance with the smart contract code. A smart contract is a computer programme that enables the creation, transfer and cancellation of tokens (see further in section I)B)2.a) below). A large number of tokens have been issued on the Ethereum Blockchain which has developed certain standards of tokens such as the "ERC-20 tokens". ERC-20 tokens are only one of the many forms of tokens that exist on the Ethereum Blockchain, and other standards of tokens exist on other blockchains. Each standard of tokens has its own specific rules and functions, which makes them compatible with different wallets or crypto-exchanges supporting these standards[20]. In light of the increasing attention of regulators worldwide to regulate the issuance of tokens, and in particular security tokens, it is worth mentioning that a new standard ERC-1400 has been developed on the Ethereum Blockchain to integrate additional functionalities specifically dedicated to security tokens and permitting for example to regulate the holding period, to whitelist and restrict the sale of tokens to non-accredited investors or put a threshold on transactions[21].

Finally, one should keep in mind that in order to transfer or effectuate transactions relating to tokens, a certain number of coins will be needed as transaction fees. For example, on the Ethereum Blockchain, a certain amount of Ethers will be used to "fuel" transactions on the Ethereum Blockchain[22] in order to send a token from one wallet to another wallet. This shows that tokens and coins are not the same thing and should therefore be distinguished.

With these clarifications on how blockchain technology functions and the role of coins and tokens, we can turn to the legal analysis of the different types of instruments based on DLT.

16 Because the public key is the only one known to the entire network, it is often referred to as the "blockchain address".

17 For additional developments, see for example, Ibid, A. Tordeurs, "Une approche pédagogique de la Blockchain", *Revue internationale des services financiers*, 2017, n°4, pp.13-14 ; *Ibid*, World Bank Group, "Distributed Ledger Technology (DLT) and Blockchain", *FinTech Note No.1*, 2017, pp.8-9.

18 ESMA, "Advice on Initial Coin Offerings and Crypto-Assets", 9 January 2019, paragraph 25.

19 "*Token vs Coin: What's the Difference*" (https://www.bitdegree.org/tutorials/token-vs-coin/).

20 "Security Tokens – An ERC-Standards Comparison", *microbo Market Research*, December 2018 (https://medium.com/@micobo/security-tokens-an-erc-standards-comparison-919e7c379f37).

21 "Security Token Standard ERC 1400 – tokenization of assets", Bitcademy, 1 May 2019 (https://medium.com/@bitcademyfb/security-token-standard-erc-1400-tokenization-of-assets-f92ba6ee6b85).

22 The term "gas" is also used to refer to the payment of a transaction fee.

2. Terminology and classification from a legal perspective

The terms "blockchain", "DLT", "coins", "tokens", "crypto-assets", "ICO", "STO" frequently appear in legal publications but it is often not clear whether they are synonyms and how they should be classified. With the clarifications made in the previous section, it is important to address these concepts from a legal perspective. However, we will not discuss their legal qualifications in detail as many authors have already done so[23].

a) the instruments: over the last few years, authors and regulators have used a wide variety of names and terminologies to refer to the instruments relying on DLT[24]. For the purpose of this analysis it seems important to clarify and somehow simplify the terminology of the different kind of instruments that the readers may come across in legal publications. Furthermore, we will briefly present the digital finance package published by the European Commission on 24 September 2020[25] with, in particular, a proposal for a regulation on markets in crypto-assets[26] ("**MiCA**") and a proposal for a regulation on a pilot regime for market infrastructure based on distributed ledger technology[27] (the "**DLT Pilot Regime**").

i) the "traditional" classification: ESMA had originally defined the term crypto-assets as "*a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT) or similar technology as part of their perceived or inherent value. Unless otherwise stated, ESMA uses the term to refer to both so-called "virtual currencies" and "digital tokens". Crypto asset additionally means an asset that is not issued by a central bank"*[28]. With that definition, ESMA introduced a dichotomy between two categories of crypto-assets, virtual currencies on one hand and digital tokens on the other hand. This corresponds to the technical distinction explained above between coins and tokens which should thus be both considered as crypto-assets from a legal perspective.

ESMA did not define the term "virtual currencies", but cross-referred to the definition[29] inserted by Directive 2018/843 of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering ("**Directive 2018/843**") and amending Directive 2015/849. Directive 2018/843 defines virtual currencies as "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or traded electronically"*[30]. Leaving aside the topic of virtual currencies which raises different legal issues, we will focus on the second category of instruments, the digital tokens.

ESMA defined the term "digital token" as "*any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use*"[31]. In addition, ESMA introduced a taxonomy[32] of the crypto-assets based on their functionalities:

(i) the "investment-type" crypto-assets that may have some profit rights attached like equities, equity-like instruments or non-equity instruments;

(ii) the "utility-type" crypto-assets that provide some utility or consumption rights; and

(iii) the "payment-type" crypto-assets which have no tangible value except for the expectation that

23 See for example: T. Bonneau, "« Tokens », titres financiers ou biens divers", Revue de droit bancaire et financier, n°1, January-February 2018 ; S. Schiller, "Blockchain- La blockchain révolutionne les levées de fonds", A*ctes pratiques & ingénierie sociétaire, n°156, November 2017* ; H. De Vauplane, "Crypto-assets, token, blockchain, ICO : un nouveau monde ? ", *Revue Banque 2017, n°810* ; M. Rousille, "Le Bitcoin : Objet juridique non identifié », *Banque et droit n°159, February 2015* ; K. Lachgar, J. Sutour, "Le token, un objet digital non identifié ?", *Option Finance n°1437, 13 November 2017, p.18* ; Dr. P. Hacker, Dr. C. Thomale, "Crypto-Securities Regulation, ICOs, Token Sales and Cryptocurrencies under EU Financial Law", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820), November 2017 ; L. Soleranski, "Réflexions sur la nature juridique des tokens", *Bulletin Joly Bourse n°03, p.191*.

24 A. Blandin, A.S. Cloots, H. Hussain, M. Rauchs, R. Saleuddin, J. Grant Allen, B. Zhang and K. Cloud, "*Global Cryptoasset Regulatory Landscape Study*", Cambridge Centre for Alternative Finance, p.34.

25 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en#:~:text=The%20strategy%20sets%20out%20four,including%20enhancing%20the%20digital%20operational.

26 https://ec.europa.eu/finance/docs/law/200924-crypto-assets-proposal_en.pdf.

27 https://ec.europa.eu/finance/docs/law/200924-distributed-ledger-technology-proposal_en.pdf.

28 ESMA, "Advice on Initial Coin Offerings and Crypto-Assets", 9 January 2019, Appendix 1.

29 The key element of that definition is that virtual currencies shall have the characteristics of "means of exchange". Recital (10) of Directive 2018/843 specifies first that virtual currencies "*should not be confused with electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC*" and second that virtual currencies can be used not only for payment or exchange but also for "*investment, store-of-value products or use in online casinos*".

30 Article 1(2)(d) of Directive 2018/843 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.

31 ESMA, "Advice on Initial Coin Offerings and Crypto-Assets", 9 January 2019, Appendix I - Glossary.

32 See also EBA, "Report with advice for the European Commission on crypto-assets", 9 January 2019, p.7.

they may serve as means of exchange or payment for goods or services external to the ecosystem in which they are built[33].

This classification has also been used by a number of authors[34]. The following developments provide a brief summary of the three types of tokens that have been traditionally recognised by legal authors and practitioners.

The first category of tokens are the investment-type tokens (or investment tokens), which are frequently referred to as security tokens or sometimes as asset tokens (although, as we will see below, such terminology should no longer be used with the introduction of the "asset-referenced tokens" to avoid any confusion between the two). Security tokens are simply tokens having the same characteristics as securities based on the definition of securities under European and/or national financial regulations. Some authors[35] have thoroughly analysed how the definition of "securities" under Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC (the "**Prospectus Regulation**") should be interpreted and applied to tokens to determine whether or not they may be deemed as securities. Since the definition of securities under the Prospectus Regulation and under Luxembourg law are substantially similar, we do not propose to repeat the analysis from a Luxembourg perspective but would like to remind the readers of the outcome of such analysis and emphasise the key elements that issuers should take into consideration when issuing security tokens.

Article 2(a) of the Prospectus Regulation defines "securities" by cross-reference to the definition of "transferable securities" as defined in article 4.1 (44) of Directive 2014/65/EU on markets in financial instruments ("**MiFID**")[36] which is as follows:

""transferable securities" means those ***classes*** *of securities which are* ***negotiable on the capital markets****, with the exception of instruments of payment, such as:*

(i) ***shares*** *in companies and all other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;*

(ii) ***bonds or other forms of securitised debt****, including depositary receipts in respect of such securities;*

(iii) any ***other securities giving the right to acquire or sell any such securities*** *or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures*;".

Based on this definition, tokens will be viewed as securities and thus considered as security tokens if (i) they are issued in a standardised form (i.e. if they all belong to the same class), (ii) they are negotiable on the capital markets (which should be understood in a broad sense) and (iii) they have characteristics similar to shares, bonds or other securities giving right to acquire shares or bonds (and to the exclusion of instruments of payments). Each of these criteria will have to be carefully analysed by issuers wishing to offer tokens to the public in order to determine whether their tokens meet the definition of securities. Security tokens like traditional securities can be further divided into two sub-categories: the equity tokens which are tokens whose rights are similar to those attached to shares (voting rights, profit entitlement, etc…), and debt tokens which are tokens whose rights are similar to bonds or securitised debt (repayment of principal and interests).

The second category of tokens are the utility tokens (also sometimes called App tokens[37]). These tokens are meant to give access to services developed by the issuer of the tokens. Certain authors[38] have made a further distinction between utility tokens and pure

33 ESMA, "Advice on Initial Coin Offerings and Crypto-Assets", 9 January 2019, paragraph 19.

34 Dr. P. Hacker, Dr. C. Thomale, "Crypto-Securities Regulation, ICOs, Token Sales and Cryptocurrencies under EU Financial Law", (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820), November 2017, p.12; P. Maume and M. Fromberger *"*Regulation of Initial Coin Offerings: Reconciling US and EU Securities Laws*", (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328064)* p.10*;* F. Annunziata, "Speak, if you can: what are you? An alternative approach to the qualification of tokens and initial coin offerings", *Bocconi Legal Studies Research Paper Series, number 2636561, February 2019*; H. Wagner, "*I*COs – Luxembourg Legal Aspects", *Les services financiers dans un monde digital, p.53*; Fondation LHoFT, "A guide through the common features of digital asset generating events", 20 May 2019 (https://www.lhoft.com/en/insights/a-guide-through-the-common-features-of-digital-asset-generating-events); K. Pauwels, A. Snyers, "Le monde merveilleux des "Initial Token Offerings" – Une première analyse d'un point de vue comptable et fiscal belge", *ACE Comptabilité, fiscalité, audit, droit des affaires au Luxembourg*, 2018/9, p.8.

35 Dr. P. Hacker, Dr. C. Thomale, "Crypto-Securities Regulation, ICOs, Token Sales and Cryptocurrencies under EU Financial Law", (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820), November 2017.

36 We note that the same definition of "securities" is used in article 1.55 of the law of 30 May 2018 on markets in financial instruments (which transposes MiFID into Luxembourg law).

37 BaFin, "Second advisory letter on prospectus and authorization requirements in connection with the issuance of crypto tokens", 22 November 2019 (https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_wa_merkblatt_ICOs_en.html).

38 K. Pauwels, A. Snyers, "Le monde merveilleux des "Initial Token Offerings" – Une première analyse d'un point de vue comptable et fiscal belge", *ACE Comptabilité, fiscalité, audit, droit des affaires au Luxembourg*, 2018/9, p.8.

utility tokens. The former category corresponds to utility tokens which intrinsically have an investment or speculative component because their value is linked to their demand on the market and thus on their utility. The latter category is different in two aspects, first because their price is fixed by the issuer and second because they can only be exchanged or traded on the platform developed by the issuer.

The third category of tokens are the payment tokens which are also sometimes referred to as currency tokens or barebone tokens[39]. These are tokens with a payment feature which constitute a means of exchange that can be used in relation to services or goods offered by the issuer of such tokens. As explained in section I)A)1.b) above, coins are typically used to pay transaction fees on a blockchain. Thus, both coins and tokens may have payment features as part of their characteristics and to avoid any confusion, it seems appropriate to refer to virtual currencies for coins associated with a particular blockchain and whose main purpose is generally the settlement of transactions solely on that blockchain, and to refer to payment tokens for tokens which have a payment feature but which resemble to vouchers or pre-paid cards that can be used to buy services or goods offered by the issuer of the tokens.

To conclude on this brief overview of the different categories of tokens, one should keep in mind that tokens may fall within more than one category[40]. The classification described above is not exclusive and in practice, tokens often have a hybrid form which renders their regulation more difficult to apprehend[41]. It is therefore important that issuers carefully consider with their counsels and/or the regulators (if any, depending on the type of issuance and structure contemplated) the features of their tokens to ensure that they comply with the relevant laws and regulations applicable to them. It is however in practice usually difficult to obtain a clean confirmation from regulators, in particular to exclude the qualification of security tokens. With the recent publication of MiCA and the DLT Pilot Regime by the European Commission, this traditional analysis of tokens split into three categories should be revisited, in particular because, as further discussed below, the three traditional categories have changed with security tokens being treated by the European Commission no differently from traditional securities and with the introduction of a new category of tokens, usually referred to as "stablecoins", which were not originally contemplated by authors. Last, one should bear in mind that the qualification of a token within the European Union may differ abroad, especially in jurisdictions having a broad definition of securities like the U.S. federal securities law with the Howey test[42]. Issuers should thus make an analysis privileging substance over form and also consider where and to whom their tokens are to be offered and traded.

ii) the impact of the proposals of new European Regulations: although MiCA and the DLT Pilot Regime remain at the stage of proposals, they constitute a major step towards the creation of a legal regime, in particular with respect to MiCA, for crypto-assets which do not fall within the scope of current European financial regulations. The objective of this paper is not to make a detailed presentation of these upcoming European regulations, which would be premature at this stage. However, the way these European regulations have been structured should be addressed.

The first remark that we would like to make is that the European Commission seems to be taking a prudent and pragmatic approach vis-à-vis the underlying technology. Recital (8) of MiCA provides that "*any legislation adopted in the field of crypto-assets should be specific, future-proof and be able to keep pace with innovation and technological developments. "Crypto-assets" and "distributed ledger technology" should therefore be defined as widely as possible to capture all types of crypto-assets which currently fall outside the scope of Union legislation on financial services*". The intent is to regulate crypto-assets but in a way that permits to capture future innovations in the field of DLT and possibly other technologies yet to be created. At the same time, the DLT Pilot Regime provides in its Recital (4) that given the limited experience of the European Union "*as regards the trading and post-trading of transactions in crypto-assets that*

39 BaFin, "Second advisory letter on prospectus and authorization requirements in connection with the issuance of crypto tokens", 22 November 2019 (https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_wa_merkblatt_ICOs_en.html).

40 See for example, ESMA "Annex 1 – Legal qualification of crypto-assets – survey to NCAs", January 2019, Appendix 1 – Overview of the six sample crypto-assets, pp-23-25.

41 Dr. P. Hacker, Dr. C. Thomale, "Crypto-Securities Regulation, ICOs, Token Sales and Cryptocurrencies under EU Financial Law", (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820), November 2017, p.33.

42 R. Dambre, "Initial Coin Offerings and U.S. Securities Regulation: Challenges and Perspectives", *International Journal for Financial Services, 2018/1*. The Howey Test refers to a ruling of the U.S. Supreme Court (*SEC v. W. J. Howey Co.*) in which it interpreted the term "investment contract", which is listed in the definition of "security" under Section 2(a)(1) of the U.S. Securities Act of 1933. According to the U.S. Supreme Court, four elements must be satisfied for a contract, transaction or a scheme to constitute an "investment contract" subject to U.S. federal securities law: (1) a person invests his money, (2) in a common enterprise, (3) is led to expect profits and (4) solely from the efforts of others. The expectation of profits is an element that is taken into consideration by U.S. law to determine whether a contract can be qualified as security. Such element has no particular bearing under European and Luxembourg law for the qualification of securities.

qualify as financial instruments, it would currently be premature to bring significant modifications to the Union financial services legislation to enable the full deployment of such crypto-assets and their underlying technology". The DLT Pilot Regime therefore suggests in the Recital (5) that "*it would be useful to create a pilot regime for DLT market infrastructures. A pilot regime for DLT market infrastructures should allow such DLT market infrastructures to be temporarily exempted from some specific requirements under the Union financial services legislation that could otherwise prevent them from developing solutions for the trading and settlement of transactions in crypto-assets that qualify as financial instruments*". These different recitals show a clear intent of the European Commission to take into account the future technological developments and not to put in place a rigid framework that would prevent innovations and business developments for Fintech actors. With respect to the DLT Pilot Regime, since it is a pilot regime, its article 10 states that ESMA shall present a report to the European Commission five years after its entry into application to present the results of this DLT Pilot Regime and in turn the European Commission shall make a report to the European Parliament and the Council to determine which actions shall be taken vis-à-vis the DLT Pilot Regime i.e. whether it shall be extended, amended or terminated. The European Commission has therefore taken a pragmatic approach which seems necessary given that these regulations are technology-oriented.

The second remark that shall be made in relation to MiCA concerns its scope which is particularly interesting as regards the classification discussed in section I)A)2.a)i) above. Recital (6) of MiCA states that "*Union legislation on financial services should not favour one particular technology. Crypto-assets that qualify as "financial instruments" as defined in Article 4(1), point (15), of Directive 2014/65/EU should therefore remain regulated under the general existing Union legislation, including Directive 2014/65/EU, regardless of the technology used for their issuance or their transfer*". Consequently, article 2.2 of MiCA excludes from its scope crypto-assets qualifying as, *inter alia*, financial instruments as defined under MiFID and electronic money as defined in Article 2, point (2) of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money.

The first legal question is therefore which crypto-assets are falling within the scope of MiCA?

First of all, MiCA defines crypto-assets as "*a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology*"[43]. As mentioned above, this definition is quite broad and not limitative in terms of technology used by the crypto-assets, and has evolved compared to the first definition of crypto-assets proposed by ESMA, as stated in section I)A)2.a)i) above. MiCA encompasses three types of crypto-assets, each of them having its regime detailed in a separate title.

The first type of crypto-asset is the utility token which is defined as "*a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token*"[44]. Recital (9) of MiCA further provides that utility tokens "*have non-financial purposes related to the operation of a digital platform and digital services*" which conversely seems to imply that if utility tokens have a financial element attached to them, then such tokens would presumably no longer qualify as utility tokens. The utility token under MiCA fully corresponds to the "utility-type" crypto-assets referred to by ESMA. Pursuant to title II of MiCA, an offer to the public of utility tokens would require the drafting of a white paper, which content and form are detailed in article 5 of MiCA, and a subsequent notification to the competent authorities with an explanation as to why the issuer considers that "*the crypto-asset described in the crypto-asset white paper is not to be considered (a) a financial instrument […]; (b) electronic money […]; (c) a deposit; (d) a structured deposit […]*"[45]. Therefore, a case-by-case analysis will remain necessary for utility tokens and the qualification exercise as to whether they may be deemed, in particular, financial instruments or electronic money will remain necessary. However, MiCA sets forth certain exemptions which will not require such white paper, including when the utility tokens will be offered for free, "*automatically created through mining as a reward*", "*unique and not fungible with other crypto-assets*" as well as the traditional exemptions to the obligation to publish a prospectus (when they will be offered to fewer than 150 natural or legal persons per Member State, the offer calculated over a period of twelve months does not exceed EUR 1,000,000 or if they are offered solely to qualified investors)[46].

43 Article 3.1(2) of MiCA.
44 Article 3.1(5) of MiCA.
45 Article 7.3 of MiCA.
46 Article 4.2 of MiCA.

The second type of crypto-asset is the asset-referenced token which is a defined as "*a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets*"[47]. Recital (9) of MiCA further explains that the asset-referenced tokens "*often aim at being used by their holders as a means of payment to buy goods and services and as a store of value*". In fact, the asset-referenced tokens are one of the two possible forms of the so-called "stablecoin"[48], the other form being the third category of tokens, the "electronic money tokens" or "e-money tokens". A stablecoin is a specific type of virtual currencies in the sense that they have a payment function and may serve as a store of value, with the specificity of being linked to an underlying asset. If the underlying asset is a currency such as a euro or a dollar, for example, the issuer of the stablecoins is supposed to hold the exact same amount of euros or dollars as the amount of stablecoins issued i.e. one stablecoin corresponding to one euro or one dollar. In other words, this means that the value of a stablecoin is perfectly aligned to the value of its underlying asset (euro or dollar in this example)[49]. As explained by a French author, one of the interests of stablecoins resides in the fact that they do not need to go through the traditional banking systems[50].

The third type of crypto-asset is therefore the second form of stablecoins, the electronic money token (e-money token). Article 3.1(4) defines them as "*a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency*". The main difference with the asset-referenced tokens is therefore the scope: the electronic money tokens are the tokens referencing only one fiat currency with legal tender (e.g. euro or dollar) whereas the asset-referenced tokens are the tokens referencing one or more fiat currencies but also one or more commodities or crypto-assets.

This paper is focusing on tokenised securities rather than virtual currencies and we therefore do not aim at making a comprehensive presentation of the asset-referenced tokens and e-money tokens here. However, for completeness, we simply note that the main requirements applicable for issuers of asset-referenced tokens will include "*the obligation to be authorised, governance requirements, rules on conflict of interests, disclosure of stabilisations mechanism, investment rules and additional white paper requirements*" while the issuers of e-money tokens "*will be subject to the regulatory requirements of the Electronic Money Directive and the rules set out in [MiCA]*"[51].

To conclude on the MiCA proposal, it is interesting to see that the paradigm of tokens has changed with this proposal. The "traditional" split of tokens between security tokens, utility tokens and payment tokens discussed in the above section, will thus evolve towards a new classification with the utility tokens and a new type of token, the so-called "stablecoins", split into asset-referenced tokens and e-money tokens. Security tokens should then be treated together with traditional securities as part of the existing European financial regulations, with the specificities that will be introduced by the DLT Pilot Regime.

The second legal question is the scope of the DLT Pilot Regime and whether it applies to all securities?

As implied by the first remark made above, the intent of this DLT Pilot Regime is not to create a specific regime for the security tokens but rather to establish "*the conditions for acquiring permission to operate a DLT market infrastructure, set[s] limitations on the transferable securities that can be admitted to trading and frame[s] the cooperation between the DLT market infrastructure, competent authorities and [ESMA]*"[52]. This DLT Pilot Regime is in other words aimed at regulating financial instruments that are traded on DLT market infrastructures which are defined as either a "*DLT multilateral trading facility*", operated by an investment firm or a market operator that only admits to trading DLT transferable securities[53], or a "*DLT securities settlement system*", operated by a central securities depository that settles transactions in DLT transferable securities against payment[54].

The DLT Pilot Regime introduces the concept of "*DLT transferable securities*" defined as transferable securities within the meaning of MiFID "*that are issued, recorded, transferred and stored using*

47 Article 3.1(3) of MiCA.
48 Recital (26) of MiCA excludes algorithmic stablecoins from the definition of asset-referenced tokens.
49 H. de Vauplane, "Les nouvelles représentations monétaires: crypto-monnaies, stablecoins, monnaies digitales des banques centrales", *Revue de droit bancaire et financier, n°3, May-June 2020*.
50 Ibid.
51 "Questions and Answers: Digital Finance Strategy, legislative proposals on crypto-assets and digital operational resilience, Retail Payments Strategy", 24 September 2020 (https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1685).
52 Ibid, "Questions and Answers: Digital Finance Strategy, legislative proposals on crypto-assets and digital operational resilience, Retail Payments Strategy", 24 September 2020.
53 Article 2(3) of the DLT Pilot Regime.
54 Article 2(4) of the DLT Pilot Regime.

DLT"[55]. This definition is interesting and should be further scrutinised in light of the distinction that can be made between tokenised securities on the one hand and security tokens on the other hand. The tokenisation process is a process through which an asset (for example a security) is recorded on DLT allowing for its registration, safekeeping and transmission. A limited number of authors have discussed this difference (or even ignored it[56]) and yet security tokens and tokenised securities are not synonyms and should not be confused. One author[57] has summarised the difference between a security token and a tokenised security by explaining that a security token is "*a new technology representation (a token) that shares some qualities with traditional securities*" whereas a tokenised security is "*a traditional asset (a security) wrapped in a new technology*". From a legal perspective this difference is important because in the case of security tokens, a qualification exercise is required to confirm whether they qualify as securities whereas in the case of tokenised securities, there is no doubt that they are securities. However, in light of these new proposals of European regulations, we can conclude that both security tokens and tokenised securities will be treated as DLT transferable securities. Security tokens are tokens which qualify as financial instruments and should be regulated as such according to MiCA. Since they are financial instruments and are by essence issued, recorded, transferred and stored using DLT, they will fall within the definition of DLT transferable securities. Tokenised securities on the other hand are securities (and therefore financial instruments) which are represented by tokens, i.e. they are wrapped together in the sense that the securities cannot be transferred without the tokens and vice versa. Despite the existence in parallel of the securities and the tokens, given that they are intertwined, with the tokens being issued, recorded, transferred and stored on DLT, they should also be treated as DLT transferable securities.

The DLT Pilot Regime will only apply to DLT transferable securities that are traded on a DLT market infrastructure. As we will further discuss in section I)B)1 below, this does not correspond to all forms of securities under Luxembourg law but will be relevant for securities in dematerialised form.

b) the offerings: the terminology associated with the offerings of tokens and coins has also been subject to a lack of clarity and some confusion was created. At first the acronym "ICO" (Initial Coin Offering) was most frequently used by authors or regulators whereas more recently the acronyms "ITO" (Initial Token Offering) or "STO" (Security Token Offering) seem to be predominantly used. However, for the reasons mentioned above, a coin offering is not the same as a token offering and a token offering is not quite the same as an offering of tokenised securities. The use of the acronym "ICO" should therefore only be appropriate in the event of an initial offering of virtual currencies which are materialised with coins, whereas the acronym "ITO" should be used if, instead of coins, tokens are being offered. The acronym "ITO" is therefore broader in scope than "STO" which refers to an offering of one particular type of token, the security tokens. Frequently, the term STO is used for an offering of tokenised securities whereas, as explained above, security tokens and tokenised securities should be distinguished.

The terminology of the offering documentation will also differ depending on the type of offer. For offers of tokens or coins, the issuer will have to draft a white paper containing, among other things, information on the issuer and the relevant participants, the characteristics of the offer, the rights and obligations attached to the crypto-assets offered, the underlying technology and the risk associated to the issuer and the crypto-assets[58]. Issuers offering tokenised securities or security tokens to the public will on the other hand have to draft a prospectus in compliance with the Prospectus Regulation and the Luxembourg law of 16 July 2019 on prospectuses, as amended (the "**Prospectus Law**"). For illustration purposes, we note that the CSSF approved on 5 July 2019 a security prospectus for subordinated token-based bonds issued by Exporo Projekt 83 GmbH. This offer corresponds to an offer of tokenised securities (in the form of subordinated bonds) but was not labelled as an STO but as a security prospectus.

The terminology used for the offering of tokens is in the end not that important[59] and is often driven by marketing and promotional considerations. However, the terminology used for the instruments is essential as the implications are not the same from a legal perspective. In the next section, we will discuss what entails an issuance of tokenised securities.

55 Article 2(5) of the DLT Pilot Regime.

56 T. Seidl, "The true value of security tokens lies in their proof of ownership – An analysis of Luxembourg securities laws and how they may be applied to serve decentralised finance solutions without the need of major changes in the laws", *ACE Comptabilité, fiscalité, audit, droit des affaires au Luxembourg, 2020/5, p.2*.

57 N. Acheson, https://www.coindesk.com/security-tokens-vs-tokenized-securities-its-more-than-semantics.

58 Article 7 of MiCA for the utility tokens, article 17 of MiCA for the asset-referenced tokens and article 46 of MiCA for the e-money tokens set out the content and form of the white papers that issuers willing to issue such types of tokens will have to comply with.

59 Unless the offer of tokens falls within the Prospectus Law.

B) Issuance of tokenised securities in the current regulatory environment

Before going into the details of the tokenisation process and the legal issues to be addressed in relation thereto, we must first discuss whether the tokenisation of securities is appropriate for all types of securities (1). Furthermore, in order to issue tokenised securities issuers will need to set up a smart contract through which the tokens will be generated and will most likely need to appoint a third party servicer with technical expertise to manage the smart contract and the tokens (2).

1. Forms of securities that can be tokenised

Under Luxembourg law, securities may be issued in three different forms: bearer form, dematerialised form or registered form. However, as we will discuss in this section, not all three forms are appropriate for tokenising securities, it being noted that specific rules have been introduced in Luxembourg law with respect to dematerialised securities.

a) bearer securities: securities in bearer form are the less common form of securities issued these days. These are the securities issued in paper form entailing that the holder of the physical certificate is the rightful owner of such securities.

In theory, securities issued in bearer form would prevent the tokenisation process to occur as it would not be possible to have at the same time securities issued in the form of physical certificate and securities represented by tokens issued on a blockchain on the other hand. It is therefore advisable that the constitutional documents of the issuer should expressly exclude the possibility to issue securities in bearer form to avoid any possible issue as regards their ownership. Furthermore, the option offered to owners of securities in registered form to convert their securities into securities in bearer form set forth in article 430-8 of the law of 10 August 1915 on commercial companies, as amended (the "**1915 Law**") should also be expressly excluded in the constitutional documents.

Yet, we note that shares in bearer form must, since the law of 28 July 2014 concerning the compulsory deposit and immobilisation of shares and units in bearer form, be deposited with a depository, which must be one of the professionals established in Luxembourg listed in article 430-6(2)[60] of the 1915 Law. Article 430-6(3) requires that the register of bearer shares be maintained by the depository in Luxembourg and indicates the mentions that it shall contain. With the consent of a depository which should have the technical capacities to play its role on the blockchain, it would therefore be possible to tokenise bearer shares once deposited, subject in addition to the conditions set out below for registered securities.

Nevertheless, this form of securities being the least frequent, a detailed presentation[61] of its regime would not be relevant whereas the second form of securities to be covered in this section is much more relevant as it is currently subject to a bill of law that would modernise its regime, including in relation to the use of DLT.

b) dematerialised securities: article 1(13) of the law of 6 April 2013 on dematerialised securities, as amended (the "**2013 Law**") defines dematerialised securities as "*an issuer's securities which are issued or converted through registration on a securities issuance account maintained by a settlement organisation or a central account keeper*". Article 1(1) of the 2013 Law defines the securities account as "*an account maintained by a settlement organisation, a central account keeper or an account keeper to which securities may be credited or debited*". Finally, article 14(1) of the 2013 Law further provides that "*the transfers between the securities account holders held with the same account keeper shall be carried out by book transfer between these accounts*". Based on these definitions, dematerialised securities are registered by way of inscription in an account specifically opened by the issuer upon issuance or conversion of dematerialised securities and which is maintained by a settlement organisation (such as Clearstream Banking S.A. in Luxembourg) or an account keeper.

On 27 July 2020, the Luxembourg government introduced a draft bill of law n°7637 (the "**Bill**") in the Luxembourg parliament in order to amend, *inter alia*, the 2013 Law. The key objective of the Bill is to modernise the 2013 Law by expressly recognising the possibility to issue and record dematerialised securities through distributed electronic ledgers or databases (being the terminology used by the Luxembourg legislator to ensure technological neutrality vis-à-vis the different types of technologies that may be used, such as DLT or blockchain). To achieve this, and in order to create more legal certainty, the Bill proposes to introduce a new definition of "issuance account" in the 2013 Law (currently, only "securities account" is defined in the 2013 Law). According to the Bill, an issuance account would be defined as an account held by a

60 This list covers a wide range of professionals from lawyers and notaries to credit institutions, portfolio managers, certain professionals of the financial sector, accountants and statutory auditors.

61 P. Dupont, P. Hoss, « La loi du 28 juillet 2014 relative à l'immobilisation des actions et parts au porteur », *Bulletin Droit & Banque 55, ALJB, 2015*.

settlement provider or central account keeper recording the dematerialised securities issued by an issuer, it being specified that such registration on an issuance account is mandatory when issuing dematerialised securities. This definition further specifies that issuance accounts may be held within or though secured electronic registration mechanisms, including distributed electronic ledgers or databases.

This Bill follows from the amendment made to the law of 1 August 2001 on the circulation of securities, as amended (the "**2001 Law**") pursuant to the law of 1 March 2019 which inserted a new article 18bis. Article 18bis (1) of the 2001 Law provides that "*the account keeper may maintain securities accounts and credit securities on securities accounts within or through secured electronic registration mechanisms, including distributed electronic ledgers or databases. Successive transfers registered within such a secured electronic registration mechanism shall be considered as book transfers between securities accounts*".

The question of the scope of this new article 18bis should be scrutinised to assess in which context the issuers may rely on this new provision to maintain and register their securities.

Article 1(1) of the 2001 Law provides that "*this law shall apply to securities in the broadest sense of the term that are deposited or held on a securities account with an account keeper and that are or have been declared fungible, be they materialised or dematerialised, in bearer, order or registered form, Luxemburgish or foreign, and regardless of the form in which they have been issued according to the law that applies to them*". Article 1(2) further provides that the 2001 Law "*shall apply exclusively to securities booked on a securities account and which are transferred by book transfer*". The definition of securities under the 2001 Law is therefore very broad and covers all types of securities whether in bearer form, registered or dematerialised form. However, article 1(2) of the 2001 Law narrows down the scope of application of the 2001 Law to the securities which are deposited or held on a securities account with an account keeper[62] and transferred by book transfer.

The definition of account keeper comes from the 2013 Law which substantially amended the provisions of the 2001 Law. The version of the 2001 Law as at 1 August 2001 had a definition of depositary (*dépositaire*) which made an express reference to credit institutions and investment firms authorised to receive securities and other financial instruments in deposit. The preparatory works of the 2013 Law confirmed that the definition of account keeper covers banks, professional securities depositaries and other types of investment firms which are authorised to hold securities accounts in accordance with Luxembourg law. We note that depending on the status of the issuer, additional regulatory constraints may come into play and limit the utility of this new article 18bis: for example, a regulated securitisation company would not be able to rely on any kind of investment firms or professional of the financial sector (e.g. a registrar agent) because the securitisation law of 22 March 2004, as amended, expressly requires that the custody of the securities be maintained by a credit institution. This amendment to the 2001 Law is therefore limited in scope and will not permit a Luxembourg issuer with securities in registered form (which are not maintained with a depositary) to rely on the new article 18bis of the 2001 Law[63].

Nevertheless, with the Bill and the 2001 Law as amended by the law of 1 March 2019, it would therefore be possible in the future to rely on DLT for maintaining both securities accounts and issuance accounts in the context of an issuance of dematerialised securities. These new provisions will be relevant mainly for securities issued by investment funds such as UCITS and kept with professionals of the financial sector in book-entry form, it being noted that these institutions only start to put in place these kind of services, which will take some time to be fully operational. These amendments to the 2001 Law and the 2013 Law will allow professionals of the financial sector to start developing financial solutions using DLT and to anticipate the entry into force of the DLT Pilot Regime which will further foster the use of DLT for financial instruments traded through market infrastructures.

For securities in dematerialised form, issuers will be able to rely on the new provisions to be inserted by the Bill and the new article 18bis of the 2001 Law as well as in the near future the DLT Pilot Regime. However, these new provisions and the DLT Pilot Regime will not be applicable to securities in registered form, which should thus be analysed separately.

c) registered securities: securities in registered form are the most common form of securities for Luxembourg corporations. These are the securities which are represented by an inscription in a register of shareholders or bondholders created to that effect. To determine whether they can be tokenised, we must first consider certain provisions of the 1915

62 Under the 2001 Law, an account keeper is "*any person authorised pursuant to the Luxembourg law to maintain securities accounts […] and active in the financial sector*".

63 B. Mathis, "La blockchain pour la circulation des titres: comparaison des régimes français et luxembourgeois", *Revue Lamy Droit des Affaires, n°144, janvier 2019, p.19*.

Law regarding the registration of shareholders and bondholders.

With respect to public limited liability companies (*société anonyme*) and corporate partnerships limited by shares (*société en commandite par actions*), article 430-3 of the 1915 Law[64] sets out the rules regarding the registers of shareholders which provide that the register of registered shares shall be maintained at the registered office of the company and that every shareholder may examine it. In terms of content, the register must specify the precise designation of each shareholder (i.e. name and address) and its number of shares, the payment made on the shares and any transfer or conversion of the shares into bearer or dematerialised shares (if allowed by the constitutional documents) and the dates of such transfers or conversions. Transfers of registered shares must be made in accordance with article 430-4 of the 1915 Law by means of a declaration of transfer entered in the register and signed by the transferor and transferee and notified to the company in accordance with article 1690 of the Luxembourg Civil Code[65].

With respect to private limited liability companies (*société à responsabilité limitée*), the rules regarding the registers of members are set in article 710-8 of the 1915 Law which simply specifies that private limited liability companies must maintain a register (without any particular indication of its localisation) which must also contain a precise designation of its members and details of the transfers of shares (*parts sociales*).

For common limited partnerships (*sociétés en commandite simples)* and special limited partnerships *(sociétés en commandite spéciales*), which are frequent in the fund industry, the rules governing the register of partners are substantially the same and must also contain, as provided in article 310-1(5) and 320-1(6) of the 1915 Law, respectively, a precise indication of the partners and record all transfers of limited partnership interests (and their date). These two provisions entitle each partner to inspect the register but the partnership agreement may provide otherwise and put in place some restrictions.

Finally, in case of issuance of bonds, notes or other type of debt securities, article 470-1[66] of the 1915 Law provides that "*a register of registered bonds shall be kept at the registered office*". The 1915 Law does not specify the content of such register but, in practice, the information contained in the register of bondholders are similar to the ones for registers of shareholders to allow the identification of the bondholders and to record the transfer of bonds. The legal documentation associated with the issuance of debt securities will typically specify the process for the registration of bondholders or noteholders and how the transfers of securities are inscribed in the register by the issuer.

In the context of the obligation set out in article 430-3 of the 1915 Law to maintain the register at the registered office of the company, discussions have been held in practice as to whether the register shall be physically maintained at all times at the registered office. Whether for the register of shares in registered form or for the register of bonds, Luxembourg law requires that such registers be maintained or kept at the registered office of the company. However, Luxembourg law does not define the concept of register and does not expressly state that it shall be maintained in paper format. Based on the 1915 Law, nothing seems to prevent the existence of a register in electronic format as long as it is maintained at the registered office of the company and, in the case of registered shares, contains the information prescribed by article 430-3 of the 1915 Law.

Legal authors[67] have already discussed the question as to whether maintaining a register in electronic format, which implies that the information of such register may be stored on different servers and thus in places other than the registered office, could be viewed as a breach of the requirement of article 430-3 of the 1915 Law[68] to maintain the register at the registered office of the company. These authors considered and concluded that the obligation of article 430-3 of the 1915 Law shall not be understood as meaning that the register must be physically located and available at all times at the registered office of the company but shall be read as an obligation on the company to ensure that the information inscribed on the register be readily accessible at any time at the registered office of the company, even though this information is stored on different servers elsewhere. To reach this conclusion, these authors relied in part on the existence of the professionals of the financial sector whose role is precisely to maintain the register of one or more financial instruments, namely the registrar agents. If such activity is permitted by article 25 of the law of 5 April 1993 on the financial sector, as amended (the "**Law of the Financial Sector**"), one should thus be able to assume that the

64 For corporate partnerships limited by shares Art. 430-3 of the 1915 Law is applicable pursuant to Art. 600-2 of the 1915 Law.

65 This is not the only way for a transfer to be entered in the register as article 430-4 of the 1915 Law further states that the inscription can be made by the company on the basis of correspondence or other documents evidencing the transfer.

66 For corporate partnerships limited by shares and public limited liability companies.

67 P. Dupont, P. Hoss, « La loi du 28 juillet 2014 relative à l'immobilisation des actions et parts au porteur », *Bulletin Droit & Banque 55, ALJB, 2015*.

68 The same analysis is applicable to registers of bondholders.

register can be maintained at a place other than the registered office, in compliance with Luxembourg law, to the extent that these transfer agents comply with the obligations imposed by the CSSF and have in place all required IT and organisational infrastructures to ensure the availability of the information on the register at all times.

The question is thus whether the analysis made in respect of registers in electronic format is transposable to registers maintained using DLT and permits issuers to comply with their obligations to maintain the relevant registers at the registered office. We see no reason to treat differently DLT registers from electronic registers, especially since the objective of DLT is to ensure the immutability and security of data (i.e. in that sense DLT registers are, at least in theory, more secured than electronic registers). However, to comply with their obligations under Luxembourg law, issuers will have to make certain arrangements, in particular in the smart contract code and the servicing agreement, as we will further discuss in section II)A)4 below.

To conclude, out of the three forms of securities under Luxembourg law, bearer securities[69] can be excluded because of their intrinsic nature that is in contradiction with the tokenisation process. Dematerialised securities can be considered for tokenisation because they benefit from a specific provision to be inserted in the 2013 Law in addition to article 18bis of the 2001 Law, which allow the registration of such securities using DLT, it being noted that the DLT Pilot Regime will complete the legal framework with further rules regarding market infrastructures. Even though dematerialised securities are currently the only form of securities that can rely on DLT-specific provisions under Luxembourg law, this does not mean that issuers will necessarily have to issue securities in dematerialised form if they want to tokenise securities[70]. Nothing in the 1915 Law prevents the issuance, transfer and recording of securities in registered form through DLT.

2. Tokenisation of securities in registered form

For the purposes of this section, we will place ourselves in the context of a tokenisation of debt securities in registered form, with tokens issued on the Ethereum Blockchain. When tokenising securities, two key contracts need to be considered, only one of which is a legal document. First of all, a smart contract must be established and tailored to the terms of the offer of tokenised securities (a). Issuers wishing to tokenise their securities will most likely need to rely on third parties with blockchain's expertise in order to perform certain functions in relation to the tokens and a contract governing their relationship should thus be entered into (b).

a) smart contract: it is important to understand what a smart contract is and how it functions because it is a critical component in the issuance of tokens.

The concept of smart contract was first introduced by Nick Szabo in its article from 1996 in which he defined a smart contract "*as set of promises, specified in digital form, including protocols with which the parties perform on these promises*"[71]. As already briefly explained in section I)A)1.b) above, a smart contract is not a traditional contract but computer code which has the particularity of automating the terms of an agreement and which is deployed on blockchain. American authors[72] have introduced an interesting distinction between two types of smart contracts. In their view, "*the code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions*". On the one hand, they qualify as "*code-only smart contracts*", the smart contracts "*that are created and deployed without any enforceable text-based contract behind them*" and, on the other hand, they qualify as "*ancillary smart contracts*" the smart contracts which are used "a*s vehicles to effectuate certain provisions of a traditional text-based contract*". This distinction presents some similarities with the distinction made above in section I)A)2.a)ii) between security tokens and tokenised securities. Security tokens are tokens which have the characteristics of securities but may not be based on a traditional contract, including in particular if the offer of such security tokens does not require the publication of a prospectus. In other words, we could have a code-only smart contract in case of a small issuance of security tokens where the parties only agree on the terms of the smart contract. On the other hand, tokenised securities are securities which are tokenised i.e. wrapped into tokens. In such a scenario, the terms of the securities are fully described in a traditional contract, or more precisely an offering document, which sets forth the terms and conditions of the securities, and the smart contract is then only used to effectuate certain actions regarding the tokens such as their transfer.

69 In paper form, i.e. which are not deposited in accordance with the law of 28 July 2014 such as bearer bonds.

70 Issuing dematerialised securities brings more constraints and additional costs for issuers, which is why they are not favoured by most commercial companies and special purpose vehicles.

71 N. Szabo, "Smart Contracts: Building Blocks for Digital Market", 1996, (https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html).

72 S. Levi and A. Lipton, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", *Harvard Law School Forum on Corporate Governance, 26 May 2018* (https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/#3b).

Although smart contracts are deployed on blockchain, it should be clarified that not all the information or data are received or validated through blockchain. This is the concept of "off-chain resources" which means that these information or data are treated outside of the blockchain. Some trusted third parties (oracles) carry out this role of retrieving "*off-chain information and then push that information to the blockchain at predetermined times*"[73].

The question remains as to the precise role of smart contracts and why issuers need to establish a smart contract when tokenising securities? Tokens are created by smart contracts and tokens cannot be operated without a smart contract, hence why securities cannot be tokenised without a smart contract. On the Ethereum Blockchain, a "*token is an entry in a register that is maintained using the smart contract. The proof that a particular distributed ledger address holds tokens is thus that the register maintained through the smart contract contains a corresponding entry*"[74]. Said differently, tokens correspond to the number of units entered into in the balance column of the blockchain register next to the blockchain addresses of the subscribers of tokenised securities. Tokens in themselves have therefore a limited interest because they are effectively only entries in a register, whereas on the other hand smart contracts are more relevant as they govern all the actions that can be taken in respect of the tokens. As already explained in section I)A)1.b) above, different standards of smart contracts have been developed by participants of the Ethereum blockchain, with the most popular smart contract being the "ERC-20" standard. Each standard of smart contract has its own specificities and functions, with some of them being of particular importance for legal practitioners. We will limit our explanations to those functionalities only[75].

Smart contracts shall set the total supply of tokens which shall match the aggregate amount of tokenised securities issued. It is indeed important to ensure that the number of tokens issued corresponds at all times with the number of securities issued (assuming a ratio of one token representing one security). The issuer may wish to issue further securities which implies that the smart contract should also be able to increase the total number of tokens in issue. The increase of the number of tokens is performed through a minter function, and from a technical perspective, we say that new tokens are "***minted***". This function can only be performed by the owner of the smart contract. As we will further discuss in section II)A)5 below, this minter function will also come into play when tokens are lost or stolen. On the other hand, the issuer may wish to redeem part of the tokenised securities issued. Smart contracts should therefore also have the opposite functionality, i.e. to reduce the total number of tokens in issue. Here, we use the terminology "***burning***" a token which consists in destroying a token from the wallet of one or several holders of tokens, which will reduce both the amount of tokens held by that particular holder as well as the total supply of tokens. This feature will also come into play when tokens are lost or stolen.

Smart contracts may permit that tokens be seized by a regulator or an authorised agent upon production of appropriate documentation. In such a case, the issuer will force the transfer of tokens to a different blockchain address indicated by the regulator or the authorised agent. Another similar function may also be put in place which is called "***killswitch***"[76] and corresponds to the situation where the issuer can force a transfer of all tokens in issue to a blockchain address controlled by it. Such functions and the context in which they can be used, should be carefully considered.

Another feature of smart contracts that is worth mentioning is the "***freeze***" function. This function, as its name suggests, allows the issuer to "*freeze the tokens, i.e. to prevent execution of transactions on the blockchain until the issuer puts an end to the freeze. This function can be used to block transactions in case of a "hard fork" of the blockchain, pending a decision of the issuer as to which version of the blockchain it will support*"[77]. We will further discuss in section II)A)3 below how issuers should anticipate the risk of hard fork from a legal perspective.

Although smart contracts are not traditional contracts, the foregoing developments illustrate why legal counsels should carefully review them and ensure that the terms and conditions of the tokenised securities described in the offering document are correctly reflected and transposed in computer language. Generally speaking, legal counsels shall ensure that the actions of the issuer permitted by the smart contract are in compliance with Luxembourg law and the constitutional and issuance documents.

73 Ibid, S. Levi and A. Lipton, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", *Harvard Law School Forum on Corporate Governance, 26 May 2018*; D. Legeais, "Blockchain", *Jurisclasseur Commercial, March 2017*.

74 Capital Markets Technology Association, "A model prospectus for the public offering of tokenized shares in Switzerland", 19 February 2020 (https://www.cmta.ch/standards).

75 For further explanations, see also Capital Markets Technology Association, "Blueprint for the tokenization of share of Swiss corporations using the distributed ledger technology", October 2018, Appendix 4.

76 Capital Markets Technology Association, "Blueprint for the tokenization of share of Swiss corporations using the distributed ledger technology", October 2018, Appendix 4, item 13.

77 Capital Markets Technology Association, "Blueprint for the tokenization of share of Swiss corporations using the distributed ledger technology", October 2018, Appendix 4, item 12.

Once the terms of the smart contracts have been agreed, smart contracts can be deployed on blockchain. To go active, smart contracts must be deployed on the relevant blockchain (Ethereum, Stellar or another one) which is a technical process corresponding to a new transaction entered on the relevant blockchain which must be validated by its participants. Once the smart contract has been deployed on the relevant blockchain, the issuer which has set a total number of tokens associated with that smart contract will assign them to the blockchain addresses (or public keys) of the investors which have subscribed to the tokens. Upon its deployment on blockchain, the smart contract will generate a unique code corresponding to a series of numbers and letters which will be publicly available. This is the smart contract address that allows investors to verify that their tokens are correctly assigned to the smart contract of the issuer.

To conclude on how smart contracts function, it must be clarified that the code of the smart contract is owned by a so-called "*default operator*" which will be the person able to interact with the tokens (not with the private keys) and who may activate the functions described above such as minting, burning or freezing tokens. The default operator has considerable powers and must therefore be either the issuer itself or an entity appointed by the issuer and acting on its behalf (the "**Servicer**"). Furthermore, the issuer or Servicer will generally have a secured and personal access to the platform where they can create and manage the tokens and which is often referred to as the "*back-end*".

b) servicing agreement: a servicing agreement for the tokens (the "**Servicing Agreement**") is generally established between the issuer and the Servicer, in particular if the issuer of the tokenised securities is a special purpose vehicle or if it lacks the adequate personnel and infrastructure to manage the tokenisation process. The object of this contract is to govern the relationship between the issuer and the Servicer which will administer the platform through which tokenised securities can be subscribed and managed.

The first type of services covered by the Servicing Agreement concerns services in relation to the on-boarding of investors willing to subscribe to tokenised securities, and in particular as regards the collection of know-your customers ("**KYC**") information[78]. KYC and anti-money laundering ("**AML**") procedures are of the utmost importance when it comes to tokens and virtual currencies because regulators are conscious that they may be a way to launder money from a criminal source. This is the reason why Directive 2018/843 has brought virtual currencies and custodian wallet providers[79] within the scope of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing. It is therefore strongly recommended that the issuer, through the Servicer, complies with KYC/AML obligations and verifies the source of the funds (especially if virtual currencies may be used to subscribe to tokenised securities). The on-boarding of investors is also a necessary step to validate their status and make sure that they meet the standards required for the offer (e.g. the offer is reserved to qualified investors in the sense of the Prospectus Regulation, or excludes US residents to avoid the triggering of U.S. federal securities laws).

The second type of services relates to the issuer's smart contract and the platform through which investors can manage their tokenised securities. Pursuant to the Servicing Agreement, the Servicer will be responsible for providing the smart contract i.e. the computer code corresponding to the terms and conditions of the securities to be tokenised, for keeping custody of the private key associated with the smart contract address, for deploying the smart contract on the relevant blockchain and allocating the tokens to the blockchain addresses of the subscribers of tokenised securities, and generally for ensuring that the platform is accessible by holders of tokenised securities on a continuous basis.

The third type of services relates to information to be exchanged between the issuer and the Servicer. The issuer shall inform the Servicer if it intends to modify or supplement the terms and conditions of the tokenised securities, in particular in case of increase or redemption of tokenised securities which, as discussed above, will require an adjustment of the total number of tokens in issue. In the event of hard fork (see further in section II)A)3 below), it shall also inform the Servicer of its decision as to which version of the blockchain it should continue to support[80]. The issuer will also provide instructions to the

78 See also, P. Lorentz, L. Bensoussan, A. Barbet-Massin, "La mise en oeuvre d'une ICO: les étapes en pratique", *Revue de droit bancaire et financier n°1, January-February 2019*.

79 Article 1(2)(d) of Directive 2018/843 defines them as "*an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies*".

80 A recent decision from a French court (*Tribunal de Commerce de Nanterre, 6ème Chambre*, 26 February 2020, case 2018F00466) illustrates the importance and necessity to anticipate carefully the risk of fork in the documentation. This matter dealt with the hard fork involving Bitcoin Cash and the legal qualification of the coins created on the blockchain resulting from the fork (the Bitcoin Cash or BCC) in the context of loans made in Bitcoins (BTC). Although we do not intend to discuss the outcome of this decision here (see for example, S. Praicheux, C. Barthout, "French court decision on the legal nature of bitcoin in the spotlight", 13 October 2020 (https://www.dlapiper.com/en/us/insights/publications/2020/10/finance-and-markets-global-insight-issue-19-2020/french-court-decision-on-the-legal-nature-of-bitcoin-in-the-spotlight/), we note that the French court used as part of its arguments

Servicer if tokens need to be minted, burnt or frozen. On the other hand, the Servicer shall immediately notify the issuer of transfers of tokens, in case a tokenholder declares through the platform (if such feature exists) that it has lost its tokens or that they have been stolen, in case of hard fork, or inform the issuer of any other event that may affect directly or indirectly the tokens.

Generally speaking, this agreement shall be drafted and adapted depending on the functionalities of the smart contract and the same has to be indicated in the terms and conditions of the tokenised securities in the offering document. In a way, this is similar to what we see with securities that are cleared through the European clearing systems and for which issuers are required to appoint, among others, an issuing and paying agent. Here the Servicer would play a role similar to an issuing and paying agent in the sense that it will provide services for deploying the tokens on a blockchain similar to how issuing and paying agents assist issuers in getting their securities deposited and cleared through the clearing systems.

II. Practical legal issues in relation to the issuance of tokenised securities

The purposes of this section is to go through the different legal issues specific to the tokenisation process that issuers will have to consider when preparing their offer of tokenised securities (A). Following the issuance and registration of the tokenised securities, further legal issues may have to be considered by issuers. The question of the transfer of tokenised securities between existing holders or to new investors will inevitably come into play and issuers and/or the Servicer should carefully consider their implication in that process. Finally, we will briefly discuss certain legal questions that will have to be answered regarding smart contracts in order to bring more legal certainty for issuers (B).

A) Legal issues arising in relation to an offer of tokenised securities

Similar to a traditional offering of securities, issuers will need to consider the scope of their offer of tokenised securities (1) and prepare the accompanying offering documentation with certain DLT-specific provisions to be included (2). In that context, issuers may want to adapt their constitutional documents to bring more legal certainty to the tokenisation process (3). Finally, issuers will need to pay particular attention to the way tokenised securities are registered (4), have procedures in place in the event that tokens are lost or stolen (5) and may consider adding certain restrictions as regards the sale and transfer of tokenised securities to avoid the application of Luxembourg and/or European financial regulations (6).

1. The scope of the offer

The first issue to consider is the structure of the offer of tokenised securities. Issuers of tokenised securities are not different from issuers of "traditional" securities and therefore need to ensure that they comply with the 1915 Law, the Prospectus Regulation or that they fall within one of its exemptions.

Depending on the amount of tokenised securities offered and/or the structure of the offer, issuers of tokenised securities may be able to rely on certain exemptions set forth in the Prospectus Regulation and the Prospectus Law. First, as regards the amount of the offer, article 1(3) of the Prospectus Regulation exempts from the obligation to publish a prospectus offers of securities to the public for a total consideration within the European Union, calculated over a 12-month period, of less than one million euros, while article 3(2) of the Prospectus Regulation and article 4(1) of the Prospectus Law exempt from the obligation to publish a prospectus offers of securities whose total consideration within the European Union, calculated over a 12-month period, is less than eight million euros, it being specified that for offers ranging between five million and eight million euros a notice of information is required pursuant to article 4(3) of the Prospectus Law. Second, the obligation to publish a prospectus will not apply if the offer meets one of the criteria set out in article 1(4) of the Prospectus Regulation, which includes in particular (to name a few) the offers to qualified investors, private placement offers (i.e. to fewer than 150 natural or legal persons per member state, other than qualified investors) or offers whose denomination per security exceeds 100,000 euros. Issuers will therefore need to carefully consider the structure of their offer of tokenised securities if they do not want to publish a prospectus satisfying the conditions of the Prospectus Regulations and the different applicable annexes, which is time-consuming and costly for issuers.

We note that the prospectus of Exporo Projekt 83 GmbH referred to under section I)A)2.b) above was approved under the old prospectus regime. The

the absence of a specific clause on the specific treatment of coins resulting from hard forks in the general terms and conditions of the crypto-exchange which granted the loans. 1,000 BTC were loaned and with the Bitcoin Cash hard fork, this resulted in the creation of 1,000 BCC on the Bitcoin Cash Blockchain. The French court had to decide whether these 1,000 BCC should be restituted to the lender as part of the loans granted in BTC, but the court ruled in favour of the borrower relying, among other things, on the absence of specific dispositions governing the attribution of coins resulting from hard fork in the general terms and conditions of the lender's crypto-exchange.

new prospectus regime with the entry into force of the Prospectus Regulation has brought additional constraints for issuers, in particular[81] as regards the risk factors section of prospectuses. In that respect, ESMA has introduced new guidelines regarding the description of risk factors in prospectuses[82], which have been thoroughly applied by the CSSF for prospectuses under the new prospectus regime. Thus, issuers willing to make a public offer of tokenised securities requiring the publication of a prospectus in accordance with the Prospectus Regulation should be aware that the CSSF will require a comprehensive disclosure of the risks, both in terms of specificity and materiality, which may not be an easy exercise for issuers of tokenised securities given the strong technological components of tokenised securities. We will describe some of them under section II)A)2.b) below.

The following developments will assume an offer of tokenised securities exempted[83] under the Prospectus Regulation and the Prospectus Law.

2. Offering document

Even if no prospectus is drawn up, an offering document will still be necessary in order to set out the terms of the offer of tokenised securities. This offering document may take different forms such as a private placement memorandum or a subscription agreement. Regardless of its form, the offering document will describe the terms and conditions of the offer of tokenised securities with certain provisions tailored to the use of DLT (a) but specific attention should also be given to the risk factors section of the offering document (b).

a) terms and conditions: the section describing the terms and conditions of the tokenised securities needs to reflect the particularities attached to the tokenisation of securities.

Unlike traditional offerings, an issuance of tokenised securities contemplates the issuance of traditional securities linked to tokens. Subscribers will only pay once (i.e. the tokens are free of charge) but the ratio securities/tokens must be expressly set out in the terms and conditions. In most cases, the ratio will be 1:1 i.e. one token issued for each security issued.

The next particularity to address in the terms and conditions is the way investors can subscribe to tokenised securities. Tokenised securities are securities wrapped into tokens which means that investors will get the tokens as a representation of their subscription to the securities rather than the securities themselves. Thus, in order to receive the relevant tokens to be issued, the investors will first need to establish a wallet that is compatible with the issuer's smart contract and the underlying blockchain. As explained in section I)A)1.a) above, wallets may come into different forms, some of them being DLT or crypto-assets' specific while other may be compatible with different DLTs and crypto-assets. This is another key element to address in the offering document which must indicate which type of wallets investors wishing to subscribe should get. The public key, which is the only way for the issuer to identify the holders of tokens on blockchain, will need to be provided by any subscriber willing to receive tokenised securities. This whole process must be explained in detail in the offering document, including the roles of wallets, private keys and public keys, as investors may not be familiar with DLT and the tokenisation of securities, and they should be fully aware of what entails the subscription of tokens.

The whole process from the subscription to the actual deployment of the tokens on blockchain should also be fully explained in the offering document, in particular when and how the tokens will be assigned to the blockchain addresses of investors. The Bitbond prospectus which was drawn up on 30 January 2019 for an issuance of "token-based bonds" (i.e. tokenised bonds) (the "**Bitbond Prospectus**")[84] may be quoted as an illustration. Condition 7.3.5 provides in substance that investors willing to subscribe to these tokenised bonds must complete a subscription form online with the number of tokens (so-called BB1-Token) they are willing to subscribe and their blockchain address (in the case of the Bitbond Prospectus, their Stellar Wallet address). Condition 7.3.5 further explains that "*the token-based bonds will be issued outside the blockchain ("Off-Chain") by accepting the subscription agreement as part of this online subscription process*" and after receipt of the payment. Finally, this Condition states that after the end of the offer period for the tokenised bonds, the tokens corresponding to the number of bonds subscribed "*will be credited immediately to the wallet of the respective investor*" i.e. the tokens will be transferred to the public key of each investor. Finally, Condition 7.3.5 concludes that "*from this point on, an investor may dispose of the BB1-Token.*

81 Prospectuses are also subject to much stricter rules as to their content which are set out in particular in Commission Delegated Regulation (EU) 2019/979 and Commission Delegated Regulation (EU) 2019/980 both dated 14 March 2019.

82 ESMA, "Guidelines on Risk factors under the Prospectus Regulation", 1 October 2019 (https://www.esma.europa.eu/sites/default/files/library/esma31-62-1293_guidelines_on_risk_factors_under_the_prospectus_regulation.pdf).

83 For a presentation of issues arising in relation to an offering of tokenised securities under the Prospectus Regulation, see for example P. Maume, "Initial Coin Offerings and EU Prospectus Disclosure", *European Business Law Review 31, n°2 (2020),* pp.185-208.

84 https://www.bitbondsto.com/files/bitbond-sto-prospectus.pdf.

The respective transaction is traceable by everyone over the Stellar Blockchain and the BB1-Token can be clearly assigned to an investor or its public key over the Stellar Blockchain".

This Condition 7.3.5 is perfectly illustrative of how the tokenisation process will operate and can be summarised as follows. Once a wallet has been created by an investor, the latter can fill out the online subscription form and make the payment for the subscription of tokenised securities (such process being carried out and verified by the issuer "off-chain"). The tokens will be assigned, at the time of the closing of the offer period, to the blockchain address of each investor who will in turn be able to dispose of such tokens. This is, of course, only illustrative and specific to the Bitbond Prospectus.

Finally, the offering document shall explain how the registration of the tokenised securities will occur and how the tokenised securities will be transferred, which we will discuss separately in section II)A)4 below.

b) risk factors[85]: A risk factors section is often included in offering documents to inform investors of certain risks associated with the issuer, the securities or the structure of the offer. With an offering of tokenised securities, it is important to warn investors about certain events or certain aspects of DLT that may affect the value of tokenised securities[86].

The first category of risks that should be mentioned are the risks associated with the tokenisation process and the fact that the securities will be wrapped into tokens. As we have seen in this paper, smart contracts are computer codes through which the tokens are issued and recorded on blockchain. Investors should be warned that technical issues affecting the smart contract such as errors, bugs or even cyber attacks on the smart contract may occur and prevent the smart contract from functioning as coded. Investors should thus be made aware that there is a risk that the smart contract ceases to operate and impairs the rights of the tokenholders.

The second category of risks relates to the type of DLT used[87]. Appropriate disclosure should be made as regards the technological risks that exist in relation to the DLT used by the issuer because one should keep in mind that most DLTs are public and open-source networks which render them vulnerable to malicious attacks, also keeping in mind that participants to a blockchain may decide collectively to amend the code and certain functionalities of the blockchain. All these risks should thus be addressed and tailored to the type of blockchain or DLT more generally. For instance, the Ethereum Blockchain, which is frequently used by issuers with tokens such as ERC-20 tokens, may be subject to cyber-attacks such as the 51% attack[88] or distributed denial of service attack[89]. Furthermore, in case of disagreement among the blockchain participants who are collaborating and developing the blockchain technology, there is a risk of hard fork which means a split of one chain of blocks into two separate chains of blocks[90]. A hard fork[91] generally occurs when the source code of the blockchain is changed and only part of the participants or nodes of the blockchain network download the update. This risk should be addressed especially if the tokens are issued on the Ethereum Blockchain since Ethereum was subject to a hard fork which resulted in a split of the blockchain between Ethereum, which was followed by the majority of participants, and Ethereum Classic which was the original source code of the blockchain[92].

The third category of risks concerns the wallets and private keys of holders of tokenised securities[93]. Investors should be warned that if their wallets were incompatible with the tokens, this would prevent the exercise of their rights over the tokens. In addition, the issuer should draw the attention of investors on

85 ESMA, "Advice on Initial Coin Offerings and Crypto-Assets", section V, 9 January 2019. Although this section addresses the risks associated with crypto-assets to be considered by regulators, it gives a useful overview of risks that should be taken into consideration by issuers.

86 For an example of risk factors section, see Capital Markets Technology Association, "A model prospectus for the public offering of tokenized shares in Switzerland" (https://www.cmta.ch/standards).

87 For an example of risk disclosure regarding the Ethereum blockchain, see for example, Capital Markets Technology Association, "A model prospectus for the public offering of tokenized shares in Switzerland", section 2.1.3.

88 A. Tordeurs, "Une approche pédagogique de la Blockchain", *Revue internationale des services financiers*, 2017, n°4, p.16.

89 The 51% attack corresponds to the situation where one miner or a pool of miners controls more than 50% of the computing power of the network and could therefore interfere with the validation of new blocks and obtain all the rewards for validating new blocks. A distributed denial of service is an attack consisting in disrupting a network by overloading the traffic on this network from multiple sources, which generally leads to malfunctions or blocking the entire network and thus preventing transactions to be recorded on blockchain.

90 As discussed in footnote 80 above, this risk is not a theoretical one and may lead to litigation to determine the rights of the parties in case of hard fork.

91 J. Lee and F. L'heureux, "A Regulatory Framework for Cryptocurrency", E*uropean Business Law Review 31, no.3 (2020): 423-446*, paragraph 1.3; World Bank Group, "Distributed Ledger Technology (DLT) and Blockchain", *FinTech Note No.1*, 2017, p.21.

92 For an explanation of the split between Ethereum and Ethereum Classic, see for example https://www.bitdegree.org/crypto/tutorials/ethereum-vs-ethereum-classic.

93 A. Blandin, A.S. Cloots, H. Hussain, M. Rauchs, R. Saleuddin, J. Grant Allen, B. Zhang and K. Cloud, "*Global Cryptoasset Regulatory Landscape Study*", Cambridge Centre for Alternative Finance, p.28.

the importance to keep their private keys in safe custody and that certain events may occur in relation to the tokens. The private keys may indeed be lost or stolen (because of a cyber-attack or malicious virus targeting the wallet software for example) which would lead to a situation where the investors would no longer be in a situation to demonstrate that they are the rightful owners of the tokens. As further discussed in section II)A)3 below, it is recommended to insert provisions in that respect in the constitutional documents of the issuer, in which case reference can made to these provisions in the risk factors section.

An additional risk disclosure that is worth mentioning for tokens issued on blockchain relates to the transaction fees that will apply for each transaction on the blockchain. As discussed in section I)A)1.a) above, blockchain functions with a system of reward in the form of coins (native of the blockchain) which are paid to the miners or the validators. These transaction fees will correspond to a payment in e.g. Bitcoin or Ether which are virtual currencies with an important volatility. It is therefore important that investors understand and take into consideration at the time of their investment that a transaction fee will apply for a transfer of tokens and that such fee may fluctuate, given the volatility of virtual currencies[94].

To conclude on the risk factors, it goes without saying that the offering document shall include a legal and regulatory risks' section. This is even more true now that the European Commission has published its proposal of regulations with MiCA and the DLT Pilot Regime. Currently, these regulations have not been adopted but we can expect that they will enter into force in the near future, together with national laws transposing them and guidelines from ESMA and national regulators. The legal and regulatory framework will therefore considerably change in the years to come, which is something that investors should be aware of as it will create more obligations for issuers, and consequently additional costs to be borne by issuers, which could eventually affect the return of investors on their tokenised securities.

3. Amendments to the constitutional documents

In the context of an issuance of tokenised securities, whether in the form of shares or bonds, it is recommended to make some amendments to the constitutional documents of the issuer[95] to ensure that provisions relating to the tokenisation process are included and thus enforceable against third parties.

First, the legal form that the underlying shares (or bonds) have is important because, as explained in section I)B)1.a) above, it would not be possible (or at least more complex) to tokenise securities if they were in bearer form. As such, it is preferable to include express wording in the constitutional documents with respect to the legal nature that the securities may have and to exclude the application of article 430-8 of the 1915 Law regarding the conversion of registered securities into bearer securities. A conversion of registered securities into dematerialised securities may also be excluded in the constitutional documents in accordance with article 430-8 of the 1915 Law but such conversion would be less problematic given the amendment made to the 2001 Law, the amendments contemplated in the Bill and the upcoming DLT Pilot Regime.

Second, it may be useful to specify that the board should be responsible for deciding of the tokenisation of securities[96] and the manner and criteria pursuant to which securities can be tokenised. This would prevent any possible discussions as to whom between the board and the general meeting should be competent for making such decision.

Third, because holders of tokenised securities are only identifiable through their public keys or blockchain addresses, it is necessary for issuers to identify them for the purposes of registering them in the relevant registers of the company. As such, it is recommended to include certain provisions in the constitutional documents specifying that information such as their blockchain address, personal identification information, and the number of tokenised securities held or subscribed be provided by each token holder[97], or at minima, delegate powers to the board to put in place the rules governing the tokenisation process[98]. This information is generally collected at the time of the on-boarding of investors, i.e. when filling out their online subscription form. An issuer may also want to request a confirmation that the tokenised securities are held on own account and not as nominee which may have an importance to ascertain the source of the funds from a KYC/AML perspective. Finally, the methods of transfer

94 J.Lee and F.L'heureux, "A Regulatory Framework for Cryptocurrency", E*uropean Business Law Review 31, no.3 (2020): 423-446*, paragraph 3.2.

95 Capital Markets Technology Association, "Blueprint for the tokenization of shares of Swiss corporations using the distributed ledger technology", October 2018, section 4.1.

96 We note that securities can be issued directly in tokenised form but it is, of course, possible to convert traditional securities in tokenised securities.

97 Capital Markets Technology Association, "Blueprint for the tokenization of shares of Swiss corporations using the distributed ledger technology", October 2018, section 4.1.3.

98 Capital Markets Technology Association, "Blueprint for the tokenization of shares of Swiss corporations using the distributed ledger technology", October 2018, Appendix 2.

of tokenised securities should also be specified with the inscription of the tokenholders as shareholders or bondholders and a notification made to the Company in accordance with article 1690 of the Luxembourg Civil Code.

Fourth, we have explained in section II)A)2.b) above that investors should be warned of the risk of hard fork of the blockchain, which is not theoretical since it occurred notably on the Ethereum Blockchain. It is, however, not sufficient to disclose this risk to investors and issuers should anticipate the occurrence of such risk. We have seen that smart contracts may contain a "freeze" function which permits to stop transactions on the register maintained on blockchain until the smart contract owner puts an end to the freeze. In that respect, the constitutional documents should take into account the risk of hard fork and include a provision expressly giving authority to the board to decide which version of the blockchain should be retained in such scenario, which would be useful to act quickly upon the occurrence of such event.

Specific provisions should also be inserted to envisage the procedures to be followed when tokens are lost or stolen, as we will discuss separately in section II)A)5 below. There is no requirement to include such procedures in the constitutional documents but the interest of doing so is that the provisions will be easily enforceable vis-à-vis third parties.

4. Registers maintained using DLT

As discussed in section I)B)1 above, the question as to whether a register can be maintained using DLT is only relevant for registered securities, which will be our focus in this section. To answer this question, it is better to take again the example of the Bitbond Prospectus[99].

The Bitbond Prospectus was made for a public offer of token-based bonds referred to as the "BB1-Tokens". Article 2 of the terms and conditions of these token-based bonds provides that the "***Issuer will generate a number of BB1-Tokens*** *equal to the number of bonds issued. One BB1-Token corresponds to EUR 1 of the issued bonds. The BB1-Tokens represent the creditors rights under the bonds set out in these Bonds Terms & Conditions and are issued to the creditors in accordance with the respective number of token-based bonds they have subscribed*". Article 1 of these terms and conditions defines the tokenholder as "*the person whose Stellar[100] address (Public Key) of its wallet is assigned to the BB1-Token present on the Stellar Blockchain*". Finally, article 4 of the terms and conditions regarding the register itself states that "*a* ***register is assigned to the smart contract of the BB1-Token on the Stellar Blockchain*** *from which all token transfers and a list of addresses holding the respective BB1-Token can be taken (the "register"). The creditors are not entered in the register by name but through their respective Blockchain addresses (public key of the wallet)*".

These definitions are useful to understand and illustrate the mechanics of tokenised securities, and in particular the fact that the holders of tokenised securities (i.e. the BB1-Tokens) will be those whose public keys (or blockchain addresses) appear on the register maintained on blockchain, it being noted that the register of tokenholders is itself assigned to the smart contract of the tokenised securities. Once the smart contract is deployed on blockchain, the register (also called ledger) will record all the transactions made in relation to the tokens, in particular, as regards the blockchain addresses of the sender and recipients of tokens as well as the relevant data associated with each transaction (i.e. the number of tokens transferred and their price). In other words, as far as tokenholders are concerned, a transfer of tokenised securities will take place only through the register maintained on blockchain.

However, issuers must take additional steps in order to comply with their obligations to maintain a register of shareholders or bondholders. If issuers solely rely on the register assigned to the smart contract and maintained on blockchain, this will not be sufficient to comply with their obligations under Luxembourg law, including because this register will contain only encrypted data with no indication of the identity of the tokenholders, the numbers of securities held, etc[101]. The question is therefore how can companies issuing registered securities in tokenised form comply with their obligations under Luxembourg law?

The first possible option is that the issuer can be one of the nodes or participants of the relevant blockchain. Since blockchain technology relies on the concept of decentralised network, it means that the issuer would in such case have a copy of the relevant ledger associated with the smart contract, permitting it to identify the tokenholders through their public keys and thus to comply with its obligations. It is important to explain that in most cases smart

99 https://www.bitbondsto.com/files/bitbond-sto-prospectus.pdf.

100 Stellar is one of the many blockchains that currently exist and is an open-source and decentralised network, particularly involved in payment transfers.

101 T. Seidl, "The true value of security tokens lies in their proof of ownership – An analysis of Luxembourg securities laws and how they may be applied to serve decentralised finance solutions without the need of major changes in the laws", *ACE Comptabilité, fiscalité, audit, droit des affaires au Luxembourg, 2020/5, section 3.2.1.*

contracts will include an interface, with specific accesses given (e.g. to the issuer, the regulator, or domiciliation agent) in order to allow an automatic match of all public keys shown on the ledger with the exact identities of the tokenholders collected during the subscription and whitelisting process.

The second possible option is to create an electronic register which is mirroring the blockchain register assigned to the smart contract. In that case, through the interface mentioned above, the issuer would be immediately notified of any transfer. In order to function properly and ensure compliance of the issuer with Luxembourg law, this functionality must be included in the smart contract, and in case of appointment of a Servicer, the Servicing Agreement must cover such services.

To conclude, we note that even though the register maintained on blockchain is accessible by all blockchain participants (assuming the blockchain used by the issuer is a public blockchain such as Ethereum), this is unlikely to cause any issue from a Luxembourg law perspective (in particular in the event of issuance of tokenised shares of a *société anonyme*, for which information on the identity of the shareholders is not public) because all the information will be encrypted through hash functions and digital signatures (public and private keys) and it will be, in theory, impossible for third parties to identify who are the holders, transferors and transferees of tokens and the object of their transactions. Only the issuer through the smart contract features will be able to decrypt this information.

5. Lost tokens and stolen tokens

As explained in the above section, tokenholders are identified by issuers through their blockchain addresses and their tokens are associated to their respective blockchain addresses. Furthermore, tokenised securities may be transferred only through a transfer of tokens. Since blockchain relies on asymmetric cryptography, the blockchain address or public key, on its own, will not be sufficient to make transactions on the tokens. Tokenholders will need their private keys to "sign" their transactions on blockchain. The following provisions are aimed at governing the situation where tokenholders no longer have control over their private key, either because they have lost it or because it has been stolen.

To protect the rights of the tokenholders vis-à-vis third parties, it is recommended that the constitutional documents include detailed procedures (similar to the following ones[102]) on how to tackle these events[103].

In the event that a tokenholder has lost access to its private key, the constitutional documents may provide that such person shall notify the issuer as soon as practicable of such loss and indicate its blockchain address so that the issuer may verify the identity of such tokenholder and ensure that it is the rightful owner of the tokenised securities. If that is the case, and to the extent that these functionalities are embedded in the smart contract, the issuer can then decide to cancel (*burn*) and re-issue (*mint*) the tokens to a new blockchain address specified by the tokenholder making that request.

In the event that a holder of tokenised securities is subject to a theft of its private key, such holder should promptly notify the issuer. The process is substantially similar to the one for lost tokens except that for private keys being stolen, there should be an additional step in order to ascertain who is the rightful owner of the tokenised securities. To do so, the constitutional documents may provide that in such a case, the issuer shall publish a notice stating that unless a holder of tokenised securities is able to provide *prima facie* evidence of its ownership of the stolen tokens, such stolen tokens will be cancelled and re-issued. If no person other than the holder of the lost tokens is claiming ownership, then the tokens that are re-issued should be allocated to such holder at the new blockchain address specified by it.

Whether or not these provisions are included in the constitutional documents, issuers should draw the attention of investors on these DLT-specific risks, and procedures to remedy the occurrence of such events should be specified in the offering document.

6. Selling and transfer restrictions

Selling and transfer restrictions are not specific to the tokenisation process but depending on the type of offers, it may be useful to adapt the offering document and the constitutional documents of the issuer.

With respect to the offering document, if tokenised securities are offered within one of the exemptions of the Prospectus Regulation (e.g. by way of private placement or to professional clients only), the issuer should include appropriate wording, standard for this kind of offering, that the tokenised securities may only be offered or sold within one exemption of the Prospectus Regulations and that the issuer has not taken any steps in any jurisdiction that would permit a public offering of the tokenised securities. Likewise, the issuer should clarify in the offering

102 These procedures are only illustrative and issuers will be able to adapt them depending on their own constraints.

103 The following procedures are taken from the work carried out by the Capital Markets Technology Association in Switzerland on the tokenisation of shares of Swiss companies. See Capital Markets Technology Association, "Blueprint for the tokenization of shares of Swiss corporations using the distributed ledger technology", October 2018, Appendix 1, section 4.

document whether it intends to have the tokenised securities listed or admitted to trading on a regulated market, a multilateral trading facility ("**MTF**") or an organised trading facility ("**OTF**") (see further in section II)B)1 below). This is the reason why the on-boarding of investors discussed in section I) B)2.b) above is important because this procedure, in theory, permits to ensure that investors subscribing to the offer of tokenised securities meet the criteria required for such offer i.e. the issuer can verify that the investors are professional clients or may set a limit of 150 natural or legal persons by member state subscribing to the offer[104].

However, the on-boarding procedure and the dispositions of the offering document may not be sufficient to prevent tokenholders from selling or transferring their tokens in a way that would put the issuer in breach vis-à-vis the Prospectus Regulation, the Prospectus Law or the securities laws of any other jurisdiction. Depending on the circumstances, it may therefore sometimes be useful to include a provision in the constitutional documents stating that in case of issuance of tokenised securities, such issuance will be strictly limited to professional clients within the meaning of Annex II of MiFID or will be made through one of the exemptions of the Prospectus Regulation or the Prospectus Law. Furthermore, and to further reduce the risks that tokenised securities are being offered to non-professional clients where the offer relies on this exemption, the issuer may expressly restrict the ownership of securities by any person whose holding would trigger the obligation to publish a prospectus or would require the issuer to hold a license or be supervised. To render these restrictions fully effective, the issuer should include additional provisions in the constitutional documents whereby the issuer would be entitled to decline the issuance of tokenised securities to such persons or their registration as tokenholders, and to require those persons to provide further information as to their legal status or decline them the right to vote at a general meeting of shareholders or bondholders (depending on the type of securities issued).

B) Legal issues arising following an issuance of tokenised securities

Once tokenised securities have been issued, legal questions may arise in relation to the trading and exchange of these tokenised securities (1). In addition, as we have seen in the preceding developments, smart contracts play a critical role for the issuance of the tokens and yet they are not regulated and may lead to certain legal issues (2).

1. Legal issues regarding secondary market activities

We do not propose to make a comprehensive analysis of the issues that may arise following an issuance of tokenised securities as it would be too broad and out of the scope of this paper[105]. Nevertheless, we would like to emphasise certain legal risks that may come into play when tokens are traded on the secondary market.

Generally, issuers of tokenised securities establish a platform (available on the internet and on smartphone) (the "**Platform**") which allows holders of tokenised securities (i.e. tokenholders) to manage their tokens directly, whether to subscribe to additional tokenised securities or to transfer them[106]. Fees may be charged by the issuer or the Servicer in relation thereto. The Platform is the interface between the tokenholders and the blockchain ledger where tokenholders will be able to trade their tokens. These arrangements may have some legal consequences as they could trigger the application of regulations such as MiFID or the Law of the Financial Sector. For the following developments, we have assumed that the issuer has not taken steps to have the tokenised securities admitted to trading on a trading venue which is already regulated.

One of the key legal risks to address is whether the Platform can be viewed as a trading venue and, in particular, an MTF or OTF. MiFID defines an MTF as "*a multilateral system operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments […] in a way that results in a contract […]*"[107] and an OTF as a "*multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract […]*"[108]. Unless the Servicer (as defined in section I)B)2.b) above) which manages the Platform is an investment firm or a market operator, we can easily exclude the qualification of MTF. We note that if the

104 For a detailed presentation of offers qualifying as public offers under the Prospectus Regulation, see P. Maume, "Initial Coin Offerings and EU Prospectus Disclosure", *European Business Law Review 31, n°2 (2020),* pp.185-208.

105 For further details, see for example, Fondation LHoFT, "A guide through the common features of digital asset generating events", 20 May 2019 (https://www.lhoft.com/en/insights/a-guide-through-the-common-features-of-digital-asset-generating-events), section VII.

106 Although we will not specifically discuss this issue here, we stress the importance of reviewing and adapting the general terms and conditions of the Platform in light of the decision of the French court discussed in footnote 80 above.

107 Article 4.1(22) of MiFID.

108 Article 4.1(23) of MiFID.

Platform were to qualify as MTF, then the DLT Pilot Regime would become relevant as it sets out specific rules and exemptions for DLT MTFs[109], which we will not address here.

However, the CSSF could consider that the Platform where the tokens are traded constitutes a multilateral system where multiple third party buying and selling interests may interact in a way that results in a contract. The definition of multilateral system[110] is sufficiently broad ("*any system or facility*") to recognise the Platform as a multilateral system. An author has scrutinised the meaning of "system" in the sense of MiFID and concluded that "*in order for a "system" to exist, it is necessary to have a set of rules (established in advance and not at the discretion of the operator) and a technical infrastructure (configurable in various ways) capable of allowing the system to function effectively*"[111]. This would be the first analysis to carry out to determine whether the Platform may qualify as a "system" in the sense of MiFID and the key element to that analysis, according to this author, will be whether a set of rules governing the functioning of such system has been defined and established. The next question is whether this multilateral system is such that third party buying and selling interests in tokenised securities (assuming they are in the form of bonds) can interact and conclude a contract.

The answer to this question is important because if the Platform were to qualify as OTF, the Servicer would have to obtain the required license from the Minister of Finance to perform such activity and would have to meet certain organisational requirements. Certain arrangements can be put in place to limit the risk of qualification of the Platform as OTF, and therefore avoid the obligations imposed on OTFs by MiFID and the Law of the Financial Sector. First, the Servicer should not play any role in the fixation of a price for the tokenised securities or receive a commission for the transactions carried out on the Platform because that could lead to the conclusion that it is actively seeking the creation of a secondary market for the tokens and provides services in relation thereto in exchange of a fee. Second, the Platform may permit tokenholders to communicate and disclose their interests in buying or selling their tokens to other tokenholders but the interface should limit such kind of interactions and not create a trading interface. In other words, it is one thing for tokenholders to negotiate via message or possibly post on a dashboard their interest in entering into a sale or purchase of tokens, and another thing to have an interface where multiple buyers and sellers can interact and thus negotiate a price among multiple counterparts. Finally, the fact that the access to the Platform may be limited to tokenholders may be another argument in favour of the exclusion of the qualification of OTF as this would limit the access of third parties' buyers.

In order to limit the risks of requalification, some European issuers consider alternative structures which fall outside the scope of European financial regulations like Switzerland or foreign countries which may have more favourable regulations for crypto-exchanges, or a clearer legal environment. This raises, however, also some risks, including the difficulty to determine technically the localisation of the Platform and the exclusion from the benefit of European regulations where by definition at least some protagonists (i.e. the issuer and/or investors) are located within the European Union, and requires a legal analysis under local law which is not always clear cut either.

Another legal risk to be considered is whether the operator of the Platform may be deemed as a broker. Article 24-1 of the Law of the Financial Sector provides that "*brokers in financial instruments are professionals whose activity consists in receiving or transmitting orders in relation to one or more financial instruments, without holding funds or financial instruments of the clients*". An authorisation from the Minister of Finance is required for such activity and appropriate organisational requirements must be put in place. Given that tokenised securities are effectively securities wrapped into a token, they could easily be qualified as financial instruments and therefore the operator of the Platform could be considered as a broker of tokenised securities if it facilitates transfers of tokens between tokenholders and receives a commission for such services.

As stated above, the role played by the Servicer should therefore be carefully considered with counsels and particular attention should also be given to any fees (whatever their form, including e.g. coins) to be paid on the Platform to limit these regulatory risks.

109 Article 2(3) of the DLT Pilot Regime defines a DLT MTF as an MTF "*operated by investment firm or market operator, that only admits to trading DLT transferable securities and that may be permitted, on the basis of transparent, non-discretionary, uniform rules and procedures, to: (a) ensure the initial recording of DLT transferable securities; (b) settle transactions in DLT transferable securities against payments; and (c) provide safekeeping services in relation to DLT transferable securities, or where applicable to related payments and collateral, provided using the DLT MTF*".

110 Article 4.1(19) of MiFID.

111 F. Annunziata, "Speak, if you can: what are you? An alternative approach to the qualification of tokens and initial coin offerings", *Bocconi Legal Studies Research Paper Series, number 2636561, February 2019*, p.47.

2. Legal issues regarding smart contracts

As we have seen throughout this paper, smart contracts play a critical role in the issuance of tokens and tokenised securities. Smart contracts, despite their name, are in essence computer programmes and therefore do not resemble civil law contracts. In the absence of definition of smart contract under Luxembourg law or at European level (and we note that neither MiCA nor the DLT Pilot Regime defines or even refers to the smart contracts in the draft proposals), it is difficult to apprehend what they are exactly from a civil law perspective and whether they should be assimilated to civil law contracts.

The difficulty with smart contracts is twofold. First, there are numerous computer codes and numerous blockchains that exist, and thus any regulation of smart contracts would need to consider this to remain technology neutral. Second, as indicated in section I)A)1.b) above, blockchain experts have started developing different standards of tokens (e.g. fungible tokens vs. non-fungible tokens) which means that different standards of smart contracts with different functionalities also exist for a particular computer code and a particular blockchain. Therefore, in addition to defining what they are, it would be useful that regulators also define their own standards and guidelines to determine whether a particular type of smart contract is subject to a specific regulation. For example, we could imagine a standard smart contract for security tokens which would be subject to the Prospectus Regulation and Prospectus Law depending on the terms of the offer.

Two additional issues can be mentioned in relation to smart contracts[112]. The first one is what is the governing law of the smart contract and which jurisdiction would be the appropriate forum in case of disputes. Unlike civil law contracts, smart contracts do not have governing law and jurisdiction clauses. However, given the intrinsic decentralised nature of blockchain technology, nodes of the network could be located in many different jurisdictions, thus leading to potential conflict of laws issues. The principles of international private law and conflicts of laws' rules could apply but it would give more legal certainty to issuers if rules regarding the governing law and jurisdiction of smart contracts were established. The second legal issue that should be mentioned is the question of the validity and legal effect of digital signatures through the cryptographic process described in section I)A)1.a) above. The technological process is secured but until they are recognised as a valid way to execute a transaction, there will be a legal risk that such transaction be considered as not being valid from a legal perspective. It would be therefore useful to define these digital signatures and give them a legal value, which could be done by reference to the Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

There are currently consultations at European level[113] to analyse these topics and one may hope that in the near future this will lead to the creation of a legal regime for smart contracts which will bring more certainty for issuers. The European Commission has already shown with MiCA and the DLT Pilot Regime that it is embracing the movement towards the digitalisation of financial services but the question of how smart contracts should be treated from a legal perspective will need to be further clarified.

112 For further discussions on legal issues arising in relation to smart contracts, see for example S. Levi and A. Lipton, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", *Harvard Law School Forum on Corporate Governance, 26 May 2018*; C. Zolynski, "Blockchain et smart contracts: premiers regards sur une technologie disruptive", *Revue de droit bancaire et financier, n°1, January 2017*.

113 Consultation on the Digital Services Act package (https://ec.europa.eu/digital-single-market/en/news/consultation-digital-services-act-package).

www.aljb.lu

B.P. 13, L-2010 Luxembourg

C.C.P.L. IBAN LU19 1111 0754 4576 0000